(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07087564 A**

(43) Date of publication of application: **31.03.95**

(51) Int. Cl **H04Q 7/38**
H04L 9/32

(21) Application number: **05182185**

(22) Date of filing: **29.06.93**

(71) Applicant: **NEC CORP**

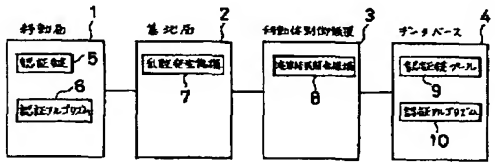
(72) Inventor: **YAHAGI MASAHIKO**

(54) AUTHENTICATION SYSTEM

(57) Abstract:

PURPOSE: To perform an authentication without the necessity of a means preliminarily storing the authentication random number and the authentication arithmetic result corresponding to each mobile station and without retrieving the authentication key of a subscriber from a data base when a subscriber authentication is performed.

CONSTITUTION: At the time of the authentication of a mobile station 1, when the mobile station 1 receives an authentication request signal from a base station 2, the station 1 performs an authentication arithmetic execution and returns an authentication response to the base station 2. When a mobile object controller 3 receives an authentication confirmation signal, the controller transmits an authentication arithmetic result request to a data base 4. The data base 4 receiving it the authentication arithmetic execution, defines the obtained authentication arithmetic result as the set parameter of the response of the authentication arithmetic result and transmits the parameter to the mobile object controller 3. The mobile object controller 3 receives the response of the authentication arithemtic result and judges that the mobile station 1 is right when a collation result coincides.



(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号

第2531354号

(45)発行日　平成８年(1996)９月４日　(24)登録日　平成８年(1996)６月27日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ　7/38			Ｈ０４Ｂ　7/26	１０９Ｓ	
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	Ａ	

請求項の数３(全 10 頁)

(21)出願番号　特願平5－182185

(22)出願日　平成５年(1993)６月29日

(65)公開番号　特開平7－87564

(43)公開日　平成７年(1995)３月31日

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　矢萩　雅彦
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　山川　政樹

審査官　清水　稔

(56)参考文献　特開　平４－233341（ＪＰ，Ａ）

(54)【発明の名称】　認証方式

(57)【特許請求の範囲】

【請求項１】　認証に使用される認証鍵、基地局より送信される認証乱数と認証鍵を入力情報として認証演算を行う認証アルゴリズムを有する移動局と、

移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて認証乱数を発生する機構、認証乱数とその認証乱数を移動局に送信し得られた認証演算結果と移動局識別番号を移動体制御装置に送出する手段を有する基地局と、

基地局より送信された移動局識別番号と認証乱数をデータベースに送信し得られた認証演算結果と基地局より送信された認証演算結果を照合する機構を有する移動体制御装置とを設け、

認証に使用する認証鍵、受信した認証乱数とその認証鍵を入力情報として認証演算を行う認証アルゴリズムと認

証演算結果を応答する機構を持つデータベースを構成要素とし基地局において認証が必要であると認識した時点で基地局で発生させた乱数を認証乱数として移動局に認証演算要求を行い、移動局より応答のあった認証演算結果を基地局において受信し、その認証乱数とその認証演算結果と移動局の識別番号を信号の設定パラメータとして移動体制御装置を基地局が起動し、

移動体制御装置において基地局より受信した信号の設定パラメータ内の認証検算結果を受信し、基地局より受信した信号の設定パラメータ内の認証演算結果とデータベースより応答のあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断することを特徴とする認証方式。

【請求項２】　請求項１において、基地局は、移動体制御装置またはデータベースにて発生させた乱数の種に基

づいて認証乱数を発生することを特徴とする認証方式。

【請求項３】　請求項１において、移動局には１つ以上の認証対象があることを特徴とする認証方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、移動体通信システムの認証方式に関するものである。

【０００２】

【従来の技術】従来の認証方式は図７に示すように移動局より親局（本発明の基地局と移動体制御装置を共に含む装置に対応）が発信要求を受け付けた時点で、親局はデータベース（本発明のデータベースに対応）に対し、識別番号（本発明の移動局識別番号に対応）を設定パラメータとして供給する。データベースは移動機認証情報を親局に返送するので、親局は移動局に対しコールプロッコ（ＣＡＬＬ　ＰＲＯＣ）信号を返答後、親局で発生させた乱数を認証乱数として移動局に送出して認証要求（本発明では認証演算要求に対応）を行い、移動局より応答のあった認証応答に含まれる認証認証演算結果を得る。

【０００３】親局はこの処理と別に移動局に送出した認証乱数を移動機認証情報により親局内で認証演算を行い、この認証演算結果と移動局より応答のあった認証応答に含まれる認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する。これは例えばＰＭＴ信号方式として、電子情報通信学会発行の信学技報（ＳＳＥ９２－７５）に記載されている。

【０００４】一方、図８および図９に示すように、複数の認証乱数とそれぞれの認証乱数に対応した複数の認証演算結果を前もって格納しておき、これを認証が必要なときに１組の認証乱数と認証演算結果として取り出し、移動局に対しその認証乱数を設定パラメータとして認証演算要求を行い、応答のあった認証演算結果と格納してあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する方式も規定されている。

【０００５】これは文献（Security Related Network Function;Recommendation GSM 03.20Version:3.3.2 Date:January 1991）に記載されており、具体的には図８においてＢＳ／ＭＳＣ／ＶＬＲが移動局の認証関連情報を必要とするとき、ＢＳ／ＭＳＣ／ＶＬＲはＨＬＲ／ＡＣに対しリクエスト（Security Related Infomatoin Reques）信号を送出する。

【０００６】ＨＬＲ／ＡＣはその信号を受信すると目的とする移動局のＫｉ（本発明の認証情報に対応）とＨＬＲ／ＡＣ内で発生した複数の乱数ＲＡＮＤ（１、２、・・・・ｎ）を入力パラメータとし、認証アルゴリズムＡ３（本発明の認証アルゴリズムに対応）に使用し、複数の認証演算結果ＳＲＥＳ（１、２、・・・・ｎ）を算出する。その後、ＨＬＲ／ＡＣ内で発生した複数の認証乱数と複数の認証演算結果はレスポンス（Authentication Vector Response）信号の設定パラメータとしてＢＳ／ＭＳＣ／ＶＬＲに応答される。

【０００７】ＢＳ／ＭＳＣ／ＶＬＲは受信した複数の乱数と複数の認証演算結果を自己の記憶装置に格納する。その後、移動局（本発明の移動局に対応）の認証が必要となったときは図９に示す様な手順で認証動作を行う。すなわちＢＳ／ＭＳＣ／ＶＬＲは対象となる移動局の１組の認証乱数ＲＡＮＤ（ｊ）および認証演算結果ＳＲＥＳ（ｊ）を選択し、ＲＡＮＤ（ｊ）を設定パラメータとして移動局に対し認証要求（Authentication Request・本発明の認証演算要求）信号を送出する。この時、移動局は自己の有する認証鍵および認証乱数（ＲＡＮＤ（ｊ））を入力パラメータとして認証演算を行い、ＢＳ／ＭＳＣ／ＶＬＲに返す。ＢＳ／ＭＳＣ／ＶＬＲは予め選択したＳＲＥＳ（ｊ）と移動局より応答のあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する。

【０００８】

【発明が解決しようとする課題】しかしながらこのような前者の認証方法では親局からデータベースへの発信情報読出要求に対する応答として発信情報読出応答信号を返し、その発信情報読出信号の設定パラメータ内に移動機認証情報を含んでいるために、親局とデータベースとの間に張られた通信回線で送受される信号を第三者が傍受することあるいは、第三者がデータベースに対して情報読出要求を送出することによって移動局番号（ＩＭＳＥ）と対応する移動機認証情報を第三者が知ることができる恐れがあった。

【０００９】また後者の認証方法ではＢＳ／ＭＳＣ／ＶＬＲ内にＢＳ／ＭＳＣ／ＶＬＲの関与する移動局毎に複数の認証乱数と対応する複数の認証演算結果を蓄積する記憶機能を有しなければならないという問題があった。

【００１０】本発明はこのような従来の課題を解決するためになされたもので、個々の移動局に対応した認証乱数と認証演算結果をあらかじめ格納する手段を必要とせず、かつ加入者認証の際、加入者の認証鍵をデータベースから引き出すことなく認証を行うようにしたものである。

【００１１】

【課題を解決するための手段】このような課題を解決するために本発明による認証方式は、移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて認証乱数を発生して移動局に認証要求を行い、移動局より送られる認証応答に含まれる認証演算結果と、認証乱数と移動局識別番号を移動体制御装置に送出する基地局と、基地局より送信された移動局識別番号と認証乱数をデータベースに送信し得られた認証演算結果と基地局より送信された認証演算結果を照合する移動体制御装置と、認証に使用する認証鍵、受信した認証

乱数とその認証鍵とを入力として認証演算を行い、認証結果を出力するデータベースとを備えている。

【００１２】

【作用】移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて基地局において認証乱数を発生し、移動局に対し認証要求を行い、認証乱数と認証対象識別番号と移動局より送られる認証応答に含まれる認証演算結果を移動局制御装置に送出し、移動体制御装置は受信した認証対象識別番号と、乱数をデータベースに送信し、得られた認証演算結果と基地局より受信した認証演算結果を照合することによって認証を行う。

【００１３】

【実施例】図１は本発明の一実施例の各構成要素が有する情報および機構を示す構成図である。移動局１は通常送信を行うことを意図するユーザによって所有され自己の装置内に認証鍵５および基地局２より送られる認証乱数と認証鍵５を入力パラメータとして認証演算を行う認証アルゴリズム６を有する。基地局２は自己の装置内に移動局１に対して認証要求を行う際、送出するに認証乱数を自律的に発生する乱数発生機構７を有する。移動体制御装置３は自己の装置内に移動局１より応答のあった認証演算結果と移動局１に対し送出した認証乱数と同一の乱数を認証乱数としてデータベース４に認証演算要求を送出することにより、得られた認証演算結果を照合する機能を持つ演算結果照合機構８を有する。

【００１４】データベース４は自己の装置内に移動局毎に異なり得る複数の移動局の認証鍵プール９と、移動体制御装置３より送られる認証乱数および同時に移動体制御装置３より送られる移動体識別番号により認証鍵プール９より得られる特定の移動局の認証鍵を入力パラメータとして認証演算を行う認証アルゴリズム１０を有する。図２は各構成要素間で転送される情報を図示したものである。基地局１２は移動局１１の認証が必要と判断した時点で自己の装置内にある乱数発生機構１７より自律的に乱数を発生する。その後、基地局１２は発生した乱数を認証乱数として、この認証乱数を設定パラメータとした移動局への認証演算要求信号２１を移動局１１に送出する。

【００１５】移動局１１は基地局１２より受信した移動局への認証演算要求信号２１内に含まれる認証乱数と自己の装置内に記憶している認証鍵１５を入力パラメータとして、自己の装置内にある認証アルゴリズム１６を使用して、認証演算を行う。その後、移動局１１は認証アルゴリズム１６によって得られた認証演算結果を設定パラメータとし、移動局からの認証応答信号２２を基地局１２に送出する。基地局１２は移動局からの認証応答信号２２を受信すると、自己の装置内で発生した乱数と移動局からの認証応答信号２２に含まれる認証演算結果と、移動局１１を示す移動局識別番号を設定パラメータとした基地局から移動体制御装置への認証確認信号２３を移動局制御装置１３へ送出する。

【００１６】移動体制御装置１３は基地局から移動体制御装置への認証確認番号２３を受信すると、その信号内に含まれる移動局識別番号と乱数を設定パラメータとした移動体制御装置からデータベースへの認証演算要求信号２４をデータベース１４に送出する。データベース１４は移動体制御装置からデータベースへの認証演算要求信号２４を受信すると、その信号内に含まれる移動局識別番号を入力パラメータとし、認証鍵プール１９をアクセスし、移動局識別番号に関連する認証鍵を得、その認証鍵と移動体制御装置１３からデータベース１４への認証演算要求信号２４に含まれる乱数を入力パラメータとし、自己の装置内にある認証アルゴリズム２０を使用して認証演算を行う。

【００１７】その後、データベース１４は認証アルゴリズム２０によって得られた認証演算結果を設定パラメータとし、データベース１４から移動体制御装置１３へ認証演算結果応答信号２５を送出する。移動体制御装置１３はデータベース１４から認証演算結果応答信号２５を受信すると、その信号内に含まれる認証演算結果を基地局１２から以前受信した移動局１１に関する認証演算結果要求信号２３に含まれる認証演算結果を自己の装置内に含まれる演算結果照合機構１８によって照合し、この照合結果が一致した場合に移動局が正当であると判断する。

【００１８】図３は移動局、基地局、移動体制御装置、およびデータベース間の信号転送タイミングと、個々の信号に含まれる主要パラメータを図示したシーケンス図である。移動局の認証が必要となったとき、基地局は乱数発生３０を行い、ここで発生した乱数を限定パラメータとし、移動局に認証要求信号３１を送出すると、移動局はパラメータに含まれる乱数を使用して、認証演算実行３２を行う。その後、移動局が認証演算実行３２によって得られた認証演算結果を設定パラメータとし、基地局に認証応答３３を送出すると、基地局は認証応答信号のパラメータに含まれる認証演算結果、基地局で発生した乱数および移動局識別番号を設定パラメータとし、認証確認信号３４を移動体制御装置に送出する。

【００１９】移動体制御装置は基地局から認証確認要求を受信すると、データベースに対してそのパラメータに含まれる乱数と、移動局識別番号を設定パラメータとし、認証演算結果要求３５を送出する。データベースは移動体制御装置から認証演算要求３５を受信すると、そのパラメータに含まれる移動局識別番号より特定の移動局に対応する認証鍵を求め、その認証鍵と認証演算要求のパラメータに含まれる乱数を用いて認証演算実行３６を行い、得られた認証演算結果を認証演算結果応答３７の設定パラメータとし、移動体制御装置に送出する。移動体制御装置は認証演算結果応答３７を受信すると、そ

のパラメータに含まれる認証演算結果と、認証確認要求３４に含まれる認証演算結果を照合し、照合結果が一致した場合に移動局が正当であると判断する。

【００２０】図１、図２、図３によって説明した認証方法を用いることにより、従来の認証方法では移動体制御装置とデータベース間に張られた通信回線で送受される信号を第三者が傍受することあるいは、第三者がデータベースに対して情報読み取り要求を送出することによって第三者が移動局識別番号に対応する認証番号を知られる恐れがあったが、この恐れを減少させることができるという効果がある。即ち、移動体制御装置とデータベースとの間に張られた通信回線で送受される信号を傍受しても知ることができる情報はある移動局に対して認証要求を行った場合の一時的な認証乱数と対応する認証演算結果の組み合わせのみであり、この組み合わせから実際の移動局に対応する認証鍵を推測することは移動局と基地局の間の通信回線を傍受する場合と同等の困難性を有する。

【００２１】また、データベース自身が公衆回線から情報読み取り要求に対応する応答機能を持たず、データベースに直接接続されている入力装置あるいは専用線によって接続されている特定の入力装置以外に情報読み取り要求を受け付けなくする構成にすることにより、第三者が移動局識別番号に対応する認証鍵を知る可能性を減少させることができる。また、この認証方式は移動体通信システムが複数の事業者によって構築された場合、移動局識別番号に対応する認証鍵が事業者間で転送されなくなる。一方、従来の認証方法では移動局の認証乱数と対応する認証演算結果を認証鍵を保持するデータベース以外の装置に蓄積する必要があり、付加的な記憶装置を必要としたが、この記憶装置を必要としない効果もある。

【００２２】図４および図５は請求項２に関連する基地局で発生する乱数の攪拌方法を示すシーケンス図である。図４において、移動体制御装置は乱数手発生４０を行い、乱数種を設定パラメータとした乱数初期化要求４１を基地局に送出する。基地局は乱数初期化要求４１を受信すると、パラメータに含まれる乱数種発生を基地局内に含まれる乱数発生機構に入力し、乱数初期化４２を行い、基地局で発生する乱数の初期化を行う。また、図５においてデータベースは乱数種発生５０を行い、乱数種設定パラメータとした乱数初期化要求５１を移動体制御装置に送出し、移動体制御装置は乱数初期化要求５１を受信すると、パラメータに含まれる乱数種を基地局に含まれる乱数種発生機構に入力し、乱数初期化５３を行い、基地局で発生する乱数の初期化を行う。

【００２３】図４、図５によって説明した認証方法を用いることにより、基地局で発生する乱数の値が繰り返される現象等が発生し、この現象を回避する必要性が生じたとき、基地局以外の構成要素の作用によって、乱数の値を変更可能となる効果がある。図６は請求項３に関連し、移動局に２つの認証対象がある場合に各構成要素間で転送される情報の一例を示すものである。基地局６３は２つの認証対象、即ち認証対象６２を有する移動局の認証が必要であると判断した時点で自己の装置内にある認証対象６１のための乱数発生機構７１および認証対象６２のための乱数発生機構７２により自律的に乱数Ａ、乱数Ｂを発生する。

【００２４】その後、基地局６３は発生した乱数Ａ、乱数Ｂをそれぞれ認証対象６１、認証対象６２への認証演算要求７５の認定パラメータとし、移動局へ認証演算要求７５を送出する。移動局は受信した認証演算要求７５の設定パラメータに含まれる乱数Ａ，Ｂをそれぞれ認証対象６１、６２に分配し、認証対象６１は認証鍵６７と、認証アルゴリズム６８と、乱数Ａ、認証対象６２は認証鍵６９と、認証アルゴリズム７０と、乱数Ｂを使用してそれぞれ独立に認証演算結果Ａ、認証演算結果Ｂを算出して、その結果を認証演算応答結果７８として送出する。基地局６３は認証演算結果応答７８を受信すると、認証確認要求７９の設定パラメータとして、認証演算結果Ａ，乱数Ａ、認証対象６１、識別番号、認証演算結果Ｂ、乱数Ｂ、識別番号を改訂し、認証確認要求７９を移動体制御装置６４へ送出する。

【００２５】移動体制御装置６４は認証確認要求７９を受信すると認証確認要求７９の設定パラメータに含まれる認証対象６１の識別番号と、乱数Ａを認証演算要求８０の改訂パラメータ、認証対象６２、識別番号と乱数Ｂを認証演算要求８２の設定パラメータとし、認証対象６１、データベース６５と認証対象６２、データベース６６に対しそれぞれ認証演算要求８０、認証演算要求８２を送出する。認証対象６１、データベース６５、認証対象６２、データベース６６は認証演算要求８０、認証演算要求８２をそれぞれ受信すると、それぞれの設定パラメータに含まれる情報を用いて独立に認証演算を行い、認証演算結果を認証演算結果応答８１、認証演算結果応答８３の設定パラメータとし、移動体制御装置６４に認証演算結果応答８３を送出する。

【００２６】移動体制御装置６４は認証対象６１、データベース６５から認証演算結果応答８１を受信すると、その設定パラメータに含まれる認証演算結果と、基地局６３から受信した認証確認要求７９に含まれる認証演算結果Ａを照合し、認証対象６１の認証を行う。同様に、認証対象６２、データベース６６から認証演算結果応答８３を受信すると、その設定パラメータに含まれる認証演算結果と基地局６３から受信した認証確認要求７９に含まれる認証演算結果Ｂを照合し、認証対象６２Ｂの認証を行う。図６によって説明した認証方法を用いることにより、移動局が複数の認証対象を有し、それぞれの認証が必要な場合、たとえば移動局の端末装置の認証と移動局を使用するユーザの認証が必要な場合においても、同様の手順で認証が行える効果があり、図１、図２、図

３の認証方法と同等の効果得られる。

【００２７】

【発明の効果】以上説明したように本発明は、基地局において認証乱数を発生し、移動局に対し認証要求を行い、認証乱数と認証対象識別番号と移動局より送られる認証応答に含まれる認証演算結果を移動局制御装置に送出し、移動体制御装置は受信した認証対象識別番号と、乱数をデータベースに送信し、得られた認証演算結果と基地局より受信した認証演算結果を照合することによって認証を行うようにしたので、データベースに含まれる認証対象の認証情報あるいは認証鍵が移動体制御装置とデータベースの間に張られた通信路内に現れず、その通信路内で送受される信号を傍受することによって認証対象の認証情報あるいは認証鍵を取得することを困難にするという効果を有し、認証対象に関連する複数の認証乱数と対応する複数の認証演算結果を複数の認証対象にわたり記憶する機構を必要としないという効果を有する。

【図面の簡単な説明】

【図１】各構成要素が有する情報及び機構を示す図である。

【図２】各構成要素間で転送される情報を示す図である。

【図３】各構成要素間の信号シーケンスを示す図である。

【図４】移動体制御装置が起動する基地局発生乱数の初期シーケンスを示す図である。

【図５】データベースが起動する基地局発生乱数の初期

化シーケンスを示す図である。

【図６】認証対象が２つある場合に各構成要素間で転送される情報を示す図である。

【図７】従来用いられている発信時の認証手順を示す図である。

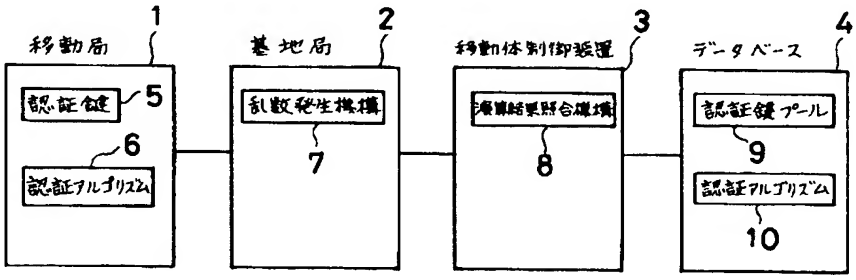
【図８】従来用いられている認証乱数および認証演算結果の格納方式を示す図である。

【図９】従来の認証手順を示す図である。

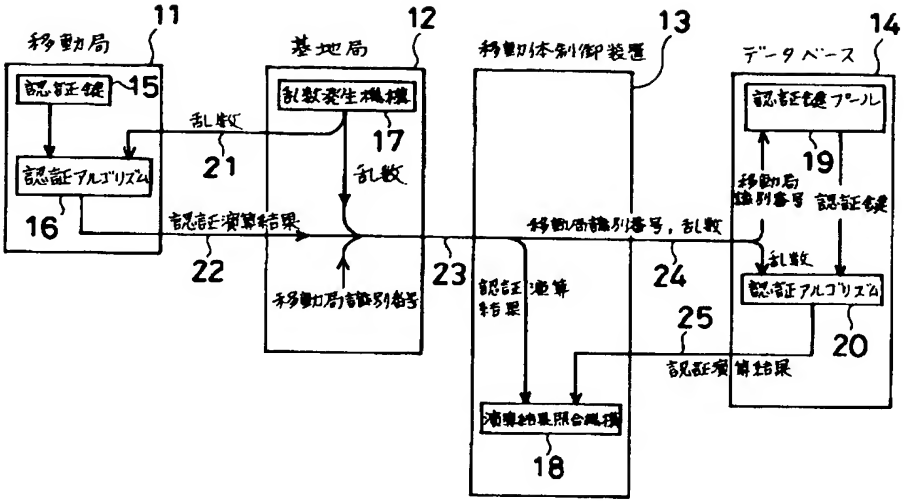
【符号の説明】

１、１１　移動局
２、１２　基地局
３、１３　移動局制御装置
４、１４　データベース
５、１５　移動局内認証鍵
６、１６　移動局内認証アルゴリズム
７、１７　乱数発生機構
８、１８　演算結果照合機構
１０、２０　データベース内認証アルゴリズム
２１　移動局への認証演算要求信号
２２　移動局からの認証応答信号
２３　基地局から移動体制御装置への認証確認要求信号
２４　移動体制御装置からデータベースへの認証演算要求信号
２５　データベースから移動体制御装置への認証結果応答信号
７５、７６、８０、８２　認証演算要求
７７、７８、８１、８３　認証演算結果応答

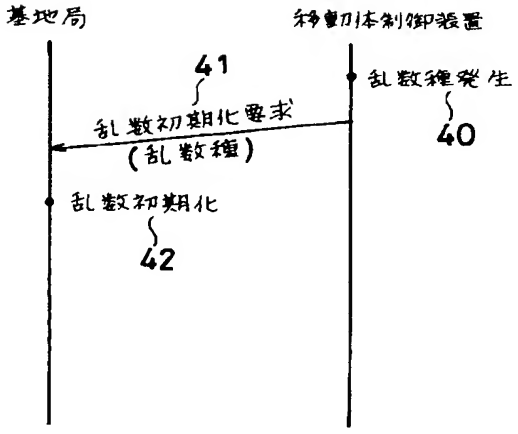
【図１】



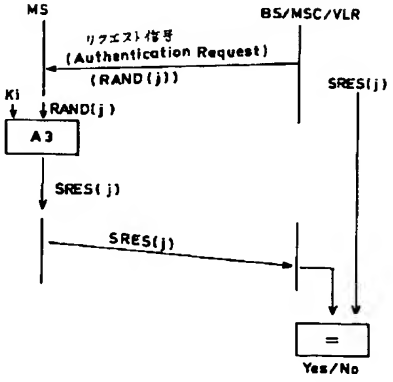
【図２】


移動局
11
認証鍵
15
認証アルゴリズム
16
基地局
12
乱数発生機構
17
乱数
21
認証演算結果
22
移動局識別番号
23
移動体制御装置
13
認証演算結果
24
25
照合結果
18
データベース
14
認証鍵プール
19
移動局識別番号
認証鍵
乱数
認証アルゴリズム
20
認証演算結果
移動局識別番号，乱数

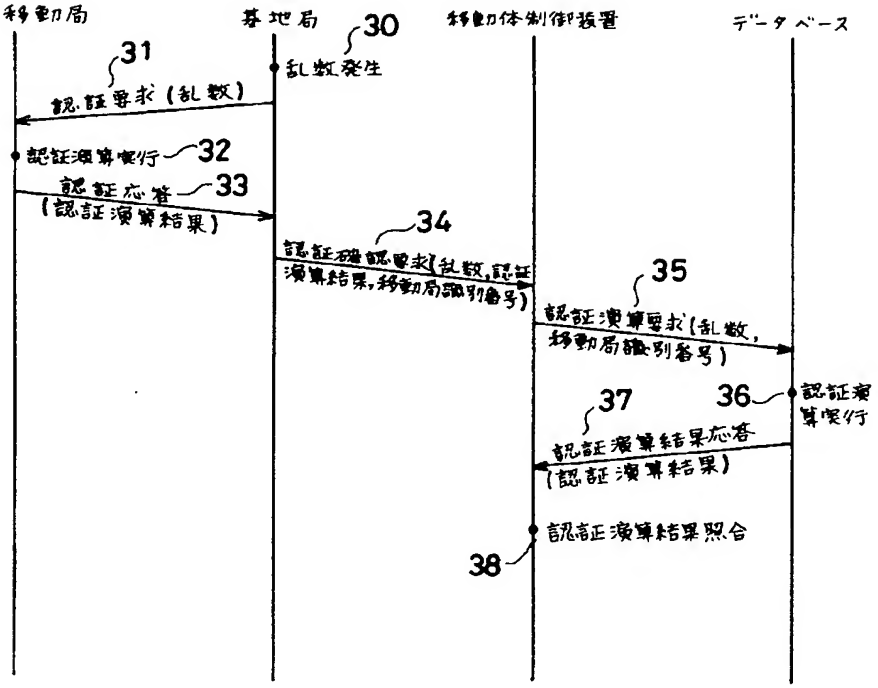
【図４】


基地局
移動体制御装置
41
乱数初期化要求
(乱数種)
乱数種発生
40
乱数初期化
42

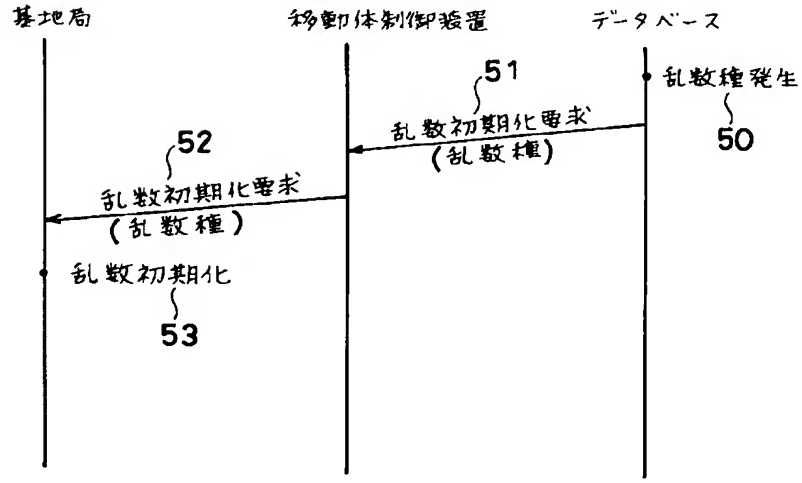
【図９】


MS
BS/MSC/VLR
リクエスト信号
(Authentication Request)
(RAND(j))
SRES(j)
Ki
RAND(j)
A3
SRES(j)
SRES(j)
=
Yes/No

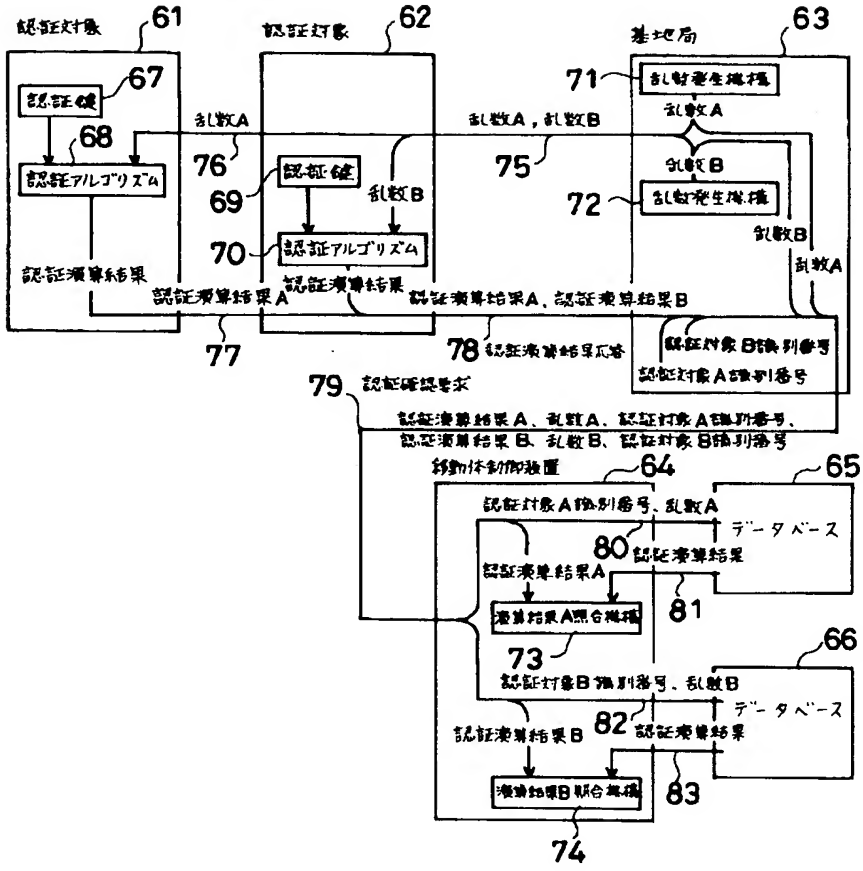
【図３】


移動局
基地局
移動体制御装置
データベース
30
乱数発生
31
認証要求（乱数）
認証演算実行
32
認証応答
33
（認証演算結果）
34
認証確認要求（乱数，認証演算結果，移動局識別番号）
35
認証演算要求（乱数，移動局識別番号）
36
認証演算実行
37
認証演算結果応答
（認証演算結果）
認証正演算結果照合
38

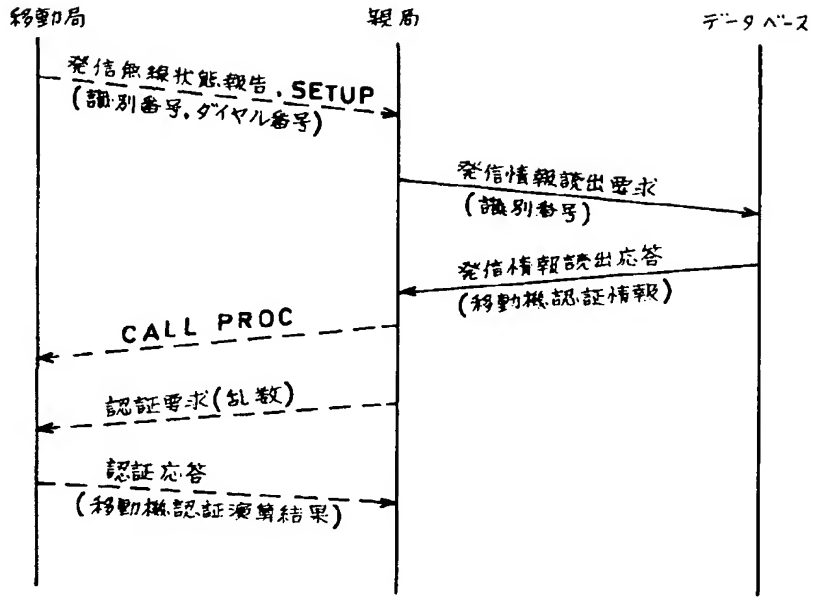
【図５】


基地局
移動体制御装置
データベース
51
乱数初期化要求
（乱数種）
乱数種発生
50
52
乱数初期化要求
（乱数種）
乱数初期化
53

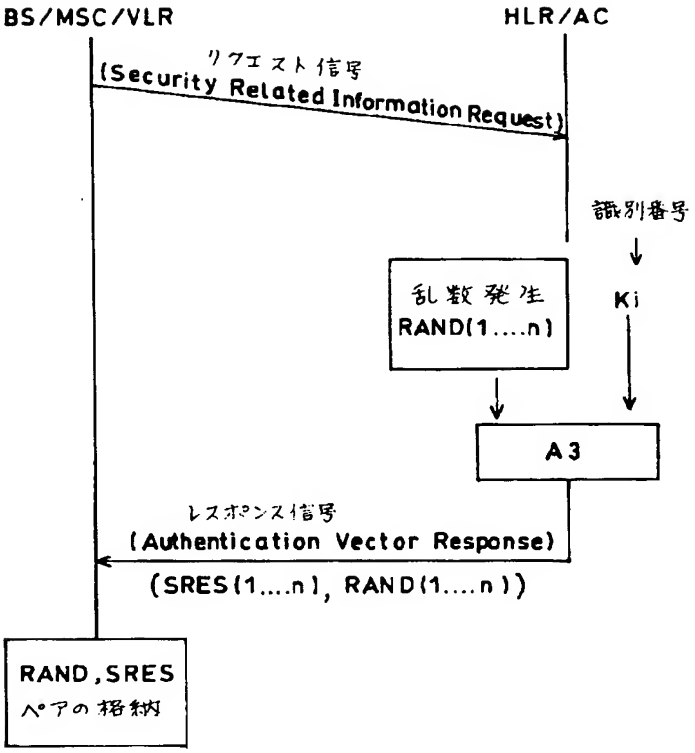
【図６】


認証対象
61
認証対象
62
基地局
63
認証鍵
67
乱数発生機構
71
乱数A
乱数A，乱数B
68
乱数A
76
75
認証アルゴリズム
認証鍵
乱数B
乱数B
69
72
乱数発生機構
乱数B
乱数A
70
認証アルゴリズム
認証演算結果
認証演算結果A
認証演算結果
認証演算結果A、認証演算結果B
77
78
認証演算結果応答
認証対象B識別番号
認証対象A識別番号
79
認証確認要求
認証演算結果A、乱数A、認証対象A識別番号、
認証演算結果B、乱数B、認証対象B識別番号
移動体制御装置
64
65
認証対象A識別番号、乱数A
データベース
80
認証演算結果
認証演算結果A
演算結果A照合機構
81
73
66
認証対象B識別番号、乱数B
データベース
82
認証演算結果B
認証演算結果
演算結果B照合機構
83
74

【図７】


移動局
親局
データベース
発信無線状態報告・SETUP
(識別番号，ダイヤル番号)
発信情報読出要求
(識別番号)
発信情報読出応答
(移動機認証情報)
CALL PROC
認証要求(乱数)
認証応答
(移動機認証演算結果)

【図８】


BS/MSC/VLR
HLR/AC
リクエスト信号
(Security Related Information Request)
識別番号
Ki
乱数発生
RAND(1....n)
A3
レスポンス信号
(Authentication Vector Response)
(SRES(1....n), RAND(1....n))
RAND, SRES
ペアの格納